Toimenpideohjelma "Turvallinen arki tietoyhteiskunnassa - ei tuurilla vaan taidolla"

Kansallisen tietoturvastrategian toteutus

Handlingsprogram
”Trygg vardag i informationssamhället
– inte med tur utan med kunskap"
Implementering av statsrådets principbeslut
om en nationell informationssäkerhetsstrategi

Action Programme
"Everyday security in the information society
- a matter of skills, not of luck"
Implementation of the Government Resolution on
National Information Security Strategy

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Helsinki, 2009

LIIKENNE- JA VIESTINTÄMINISTERIÖ

KUVAILULEHTI

Julkaisun päivämäärä

28.12.2009

Tekijät (toimielimestä: toimielimen nimi, puheenjohtaja, sihteeri)	Julkaisun laji
Arjen tietoyhteiskunnan neuvottelukunnan alainen	Toimenpideohjelma
tietoturvallisuusryhmä	Toimeksiantaja Liikenne- ja viestintäministeriö
Pj. Mari Herranen, siht. Mirka Meres-Wuori	Toimielimen asettamispäivämäärä

Julkaisun nimi

Toimenpideohjelma "Turvallinen arki tietoyhteiskunnassa - ei tuurilla vaan taidolla". Kansallisen tietoturvastrategian toteutus.

Tiivistelmä

Kansallisen tietoturvastrategian tavoitteiden saavuttamiseksi hyväksyttiin toimenpideohjelma marraskuussa 2009. Toimenpideohjelma laadittiin vuoden 2009 aikana arjen tietoyhteiskunnan neuvottelukunnan alaisessa tietoturvallisuusryhmässä. Toimenpideohjelman keskeisenä ajatuksena on, että siinä toimeenpannaan muutamia keskeisiä hankkeita, joilla ratkaisevasti edistetään tietoturvaa Suomessa ja saadaan siten kansallinen tietoturvastrategia toteutettua tehokkaasti. Tarkoituksena on hakea synergioita ja miettiä tarkasti missä asioissa voidaan tuottaa lisäarvoa. Toimenpideohjelmalla on myös rajapintoja muiden ohjelmien kanssa, jotka otetaan työssä huomioon.

Toimenpideohjelmaan on koottu strategian pohjalta 9 kärkihanketta, joissa paneudutaan uusiin ajankohtaisiin tietoturva-asioihin, parannetaan olemassa olevia toimintoja sekä vältetään päällekkäisten toimintojen tekemistä. Jokaiselle hankkeelle on nimetty vetäjä sekä muut osallistuvat tahot. Hankkeille luodaan vetovastuullisten johdolla mittarit, joiden avulla hankkeen toteutumista seurataan.

Toimenpideohjelma pohjautuu valtioneuvoston periaatepäätökseen kansallisesta tietoturvastrategiasta ”Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla –”, joka hyväksyttiin joulukuussa 2008. Strategian tavoitteena on luoda suomalaisille (kansalaiset, yritykset, viranomaiset ja muut toimijat) turvallinen arki tietoyhteiskunnassa. Strategian visiona on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa. Strategiassa on kolme painopistealuetta; 1) Perustaidot arjen tietoyhteiskunnassa, 2) Tietoihin liittyvien riskien hallinta ja toimintavarmuus, sekä 3) Kilpailukyky ja kansainvälinen verkostoyhteistyö.

Avainsanat (asiasanat)

tietoturva

Muut tiedot

Yhteyshenkilö/LVM Mari Herranen

Sarjan nimi ja numero	ISSN	ISBN
Liikenne- ja viestintäministeriön julkaisuja 51/2009	1457-7488 (painotuote) 1795-4045 (verkkojulkaisu)	978-952-243-127-1 (painotuote) 978-952-243-128-8 (verkkojulkaisu)

Sivumäärä (printti)	Kieli	Hinta	Luottamuksellisuus
44	suomi		julkinen

Jakaja	Kustantaja
Liikenne- ja viestintäministeriö	Liikenne- ja viestintäministeriö

KOMMUNIKATIONSMINISTERIET

PRESENTATIONSBLAD

Utgivningsdatum

28.12.2009

Författare (uppgifter om organet: organets namn, ordförande, sekreterare)	Typ av publikation
Gruppen för informationssäkerheten i vardagens	Handlingsprogram
informationssamhälle	Uppdragsgivare Kommunkationsministeriet
Ordförande Mari Herranen, sekreterare Mirka Meres-	Datum för tillsättandet av organet

Publikation

Handlingsprogram ”Trygg vardag i informationssamhället – Inte med tur utan med kunskap"; implementering av statsrådets principbeslut om en nationell informationssäkerhetsstrategi

Referat

För att uppnå målen i statsrådets principbeslut om en nationell informationssäkerhetsstrategi så godkändes handlingsprogrammet i november 2009. Handlingsprogrammet har beretts i gruppen för informationssäkerhet under delegationen för vardagens informationssamhälle. Den bärande tanken i handlingsprogrammet är att genomföra ett antal projekt som på ett avgörande sätt kan främja informationssäkerheten i Finland och bidra till att den nationella informationssäkerhetsstrategin blir effektivt genomförd. Meningen är att söka synergier och noga se på vilka frågor som kan ge ett mervärde. Handlingsprogrammet tangerar också andra program och de ska vägas in i arbetet.

Utifrån strategin har 9 nyckelprojekt sammanställts i handlingsprogrammet. De ska ta upp nya aktuella informationssäkerhetsfrågor, förbättra existerande funktioner och undvika överlappningar. För varje projekt har det utsetts en projektansvarig och andra deltagare. De ansvariga ska se till att det tas fram indikatorer att följa upp projekten med.

Statsrådets principbeslut om en nationell informationssäkerhetsstrategi ”Trygg vardag i informationssamhället – Inte med tur utan med kunskap" godkändes av statsrådet i december 2008. Med hjälp av den nationella informationssäkerhetsstrategin strävas det efter att skapa finländarna (medborgare, företag, myndigheter och andra aktörer) en trygg vardag i informationssamhället. Strategin har den visionen att medborgarna och företagen kan lita på att deras uppgifter är säkra både på data- och kommunikationsnäten och i tjänsterna som hör till dem. Strategin har tre tyngdpunkter; 1) Baskunskaper i vardagens informationssamhälle, 2) Riskhantering som anknyter till information och funktionssäkerhet, och 3) Konkurrenskraft och internationellt nätverkssamarbete.

Nyckelord

informationssäkerhet

Övriga uppgifter

Kontaktperson vid ministeriet är Mari Herranen.

Seriens namn och nummer	ISSN	ISBN
Kommunikationsministeriets publikationer 51/2009	1457-7488 (trycksak) 1795-4045 (nätpublikation)	978-952-243-127-1 (trycksak) 978-952-243-128-8 (nätpublikation)

Sidoantal (nätpublikation)	Språk	Pris	Sekretessgrad
44	finska		offentlig

Distribution	Förlag
Kommunikationsministeriet	Kommunikationsministeriet

MINISTRY OF TRANSPORT AND COMMUNICATIONS FINLAND

DESCRIPTION

Date of publication

28 December 2009

Authors (from body; name, chairman and secretary of the body)	Type of publication
Information Security Group of the Ubiquitous	Action Programme
Information Society Advisory Board	Assigned by Ministry of Transport and Communications
Chairman Mari Herranen, secretary Mirka Meres-Wuori	Date when body appointed

Name of the publication

Action Programme "Everyday security in the information society - a matter of skills, not of luck"; implementation of the Government Resolution on National Information Security Strategy

Abstract

In order to attain the National Information Security Strategy's goals, an action programme was approved in November 2009. The action programme was formulated during year 2009 by the Information Security Group, which works under the Ubiquitous Information Society Advisory Board. A key idea of the action programme is that it will execute several key projects that will decisively promote information security in Finland and thus effectively implement the National Information Security Strategy. The intention is to seek synergies and consider precisely in which areas added value can be generated. The action programme also has interfaces with other programmes, which will be taken into account in the work.

Based on the strategy, the action programme brings together nine key projects, which will address new topical information security issues, improve existing work and avoid overlapping measures. A leader and other participants have been appointed for each project. Under the direction of those in positions of responsibility, indicators will be created for the projects to aid in monitoring their implementation.

The Government Resolution on National Information Security Strategy "Everyday security in the information society - a matter of skills, not of luck", was adopted by the Finnish Government in December 2008. The aim of the National Information Security Strategy is to make everyday life in the information society safe and secure for everyone in Finland – for people as individuals and for businesses, administrative authorities, and all other actors in society. The Strategy's vision is that people and businesses will be able to trust that their information is secure when it is processed in information and communications networks and related services. There are three priority areas in the Strategy; 1) Basic skills in the ubiquitous information society, 2) Information risk management and process reliability, and 3) Competitiveness and international network cooperation.

Keywords

information security

Miscellaneous

Contact person at the Ministry Ms. Mari Herranen

Serial name and number	ISSN	ISBN
Publications of the Ministry of Transport and Communications 51/2009	1457-7488 (printed version) 1795-4045 (electronic version)	978-952-243-127-1 (printed version) 978-952-243-128-8 (electronic version)

Pages, total (printed version)	Language	Price	Confidence status
44	Finnish		Public

Distributed and published by

Ministry of Transport and Communications

"TURVALLINEN ARKI TIETOYHTEISKUNNASSA – EI TUURILLA VAAN TAIDOLLA"

VALTIONEUVOSTON PERIAATEPÄÄTÖS KANSALLISEKSI TIETOTURVASTRATEGIAKSI 4.12.2008

TOIMENPIDEOHJELMA

Sisältö:

1. JOHDANTO

Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi hyväksyttiin joulukuussa 2008. Kansallisen tietoturvastrategian tavoitteena on luoda suomalaisille (kansalaiset, yritykset, viranomaiset ja muut toimijat) turvallinen arki tietoyhteiskunnassa. Strategian visiona on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa.

Edellisen tietoturvastrategian aikana tietoturvatyö saatettiin käyntiin Suomessa laajalla rintamalla. Vuonna 2003 julkaistu tietoturvastrategia oli Suomessa ja Euroopassa ensimmäinen laatuaan. Uuden strategian ja siihen pohjautuvan toimenpideohjelman tavoitteena on keskittyä muutamiin alan asiantuntijoiden keskeisimpinä pitämiin kehittämiskohteisiin ja saada niissä aikaan mahdollisimman konkreettisia tuloksia.

Toimenpideohjelman valmistelu on tehty arjen tietoyhteiskunnan neuvottelukunnan alaisessa tietoturvallisuus – ryhmässä. Ryhmän tehtävänä on edistää tietoyhteiskunnan tietoturvallisuutta, seurata tietoturvallisuuden kehittymistä sekä tehdä aloitteita tietoturvallisuuden parantamiseksi. Ryhmään kuuluu yli 20 julkisen ja yksityisen sektorin tietoturvavaikuttajaa. Toimenpideohjelma on valmisteltu kansallisen tietoturvastrategian tavoitteiden saavuttamiseksi periaatepäätöksen painopisteiden pohjalta.

Toimenpideohjelman valmistelu on pyritty pitämään mahdollisimman avoimena prosessina. Toimenpideohjelman koostamisen pohjaksi järjestettiin laaja lausuntokierros uudesta tietoturvastrategiasta sekä avattiin asiasta julkinen keskustelu otakantaa.fi sivustolla. Tietoturvallisuus -ryhmä on valmistelun aikana kokoontunut neljä kertaa ja järjestänyt strategiaseminaarin ja työpajan tietoturvapäivänä 10.2.2009. Luonnos toimenpideohjelmaksi oli laajalla lausuntokierroksella 2009 aikana. Tietoturvallisuusryhmän sisällä on lisäksi toiminut erillinen toimenpideohjelmaa valmisteleva työvaliokunta.

Toimenpideohjelman keskeisenä ajatuksena on, että siinä toimeenpannaan muutamia keskeisiä hankkeita, joilla ratkaisevasti edistetään tietoturvaa Suomessa ja saadaan siten kansallinen tietoturvastrategia toteutettua tehokkaasti. Tarkoituksena on hakea synergioita ja miettiä tarkasti missä asioissa voidaan tuottaa lisäarvoa. Toimenpideohjelmalla on myös rajapintoja muiden ohjelmien kanssa, jotka otetaan työssä huomioon (mm. eräät sisäasiainministeriön sisäisen turvallisuuden ohjelmaan kuuluvat hankkeet). Valtionvarainministeriön strategiatyössä ja sen jalkauttamisessa keskitytään valtionhallinnon tietoturvallisuuteen.

Toimenpideohjelmaan on koottu strategian pohjalta 9 kärkihanketta, joissa paneudutaan uusiin ajankohtaisiin tietoturva-asioihin, parannetaan olemassa olevia toimintoja sekä vältetään päällekkäisten toimintojen tekemistä. Jokaiselle hankkeelle on nimetty vetäjä sekä muut osallistuvat tahot (mukana ainakin mainitut tahot). Hankkeille luodaan vetovastuullisten johdolla mittarit, joiden avulla hankkeen toteutumista seurataan. Toimenpideohjelman koordinointivastuu on arjen tietoyhteiskunnan tietoturvallisuus -ryhmällä.

2. PERUSTAIDOT ARJEN TIETOYHTEISKUNNASSA

*Ensimmäisen painopisteen toimenpiteissä kehitetään kansallista tietoturvapäivä-hanketta, lisätään tietoturvatietoisuutta, seurataan tietoisuuden tasoa ja kehitetään tietoturvaosaamista, laaditaan aktiivinen ja ennakoiva viestintäsuunnitelma. Lisätään tietoturvavaatimukset osaksi jokaista tarjouspyyntöä, ml. ratkaisujen ja palvelujen suunnitteluvaiheet, edistetään tietoturvaratkaisujen laajempaa käyttöä, selvitetään mahdollisuutta kehittää turvallisille palveluille myönnettävää erillistä sertifikaattia, edistetään sertifioitujen tietoturva-ammattilaisten määrän lisäämistä Suomessa. **

HANKE 1: Tietoturvatietoisuuden lisääminen

Tausta/ toimenpiteen sisältö:

Toimiva tietoyhteiskunta edellyttää, että sen tarjoamien palveluiden turvallisuus pystytään takaamaan. Tietoturva on kaikkien tietoyhteiskuntaan osallistuvien vastuulla ja jokaisen tahon on ymmärrettävä oma osuutensa tästä vastuunjaosta. Tämän takia on erityisen tärkeää kasvattaa tietoturvaymmärrystä kaikkialla yhteiskunnassa.

Hankkeessa arvioidaan, mitä tietoturvan perustaidot arjen tietoyhteiskunnassa tarkoittavat ja tämän pohjalta valmistellaan tietoturvaviestejä kaikille keskeisille väestöryhmille. Viestien jalkauttamiseksi valmistellaan erillinen viestintäsuunnitelma.

Hankkeessa arvioidaan lisäksi Tietoturvapäivä -konseptin kehittämistarpeet, joista keskeisimpänä on tietoturvapäivän laajentaminen koko maata koskevaksi. Tietoturvapäivähankkeessa pyritään saamaan tietoturvapäivän tilaisuuksia pääkaupunkiseudun lisäksi myös alueelliselle ja paikalliselle tasolle. Vuosittain helmikuussa järjestettävä tietoturvapäivä on julkishallinnon, elinkeinoelämän ja järjestöjen yhteinen hanke ja sen tarkoituksena on kansalaisten tietoturvatietoisuuden lisääminen.

Hankkeessa tulee huomioida erityisesti pk-sektori siten, että selvitetään mahdollisuudet luoda oma tietoturvahanke pk-sektorille. Pk-yrityksille suunnatussa tietoturvaviestinnässä tulee ottaa huomioon nykyistä paremmin yritysten tarpeet teknisten näkökohtien korostamisen sijaan. Tietoturvaviestit tulee liittää tiiviiksi osaksi yritysten liiketoimintanäkökulmaa.

Suomalainen koulujärjestelmä on pohja kansalliselle tietoturvaosaamiselle. Tietoturvaopetus tulee varmistaa kaikille koululaisille ja opiskelijoille ja se pitää laajentaa myös ATK-opetuksen ulkopuolelle. Hankkeessa pyritään vaikuttamaan siihen, että tietoturvavalmiuksia kehitetään jokaisella koulutusasteella.

Tulos /vaikuttavuustavoite:

Yleistavoitteena on kansallisen tietoturvatietoisuuden parantuminen sekä tietoturvaan liittyvien vastuiden, oikeuksien ja velvollisuuksien selkeytyminen. Tietoyhteiskunta on mahdollistanut useiden arjen askareiden ja toimien hoitamisen monipuolisesti verkossa, joten siellä tulee noudattaa samoja sääntöjä ja turvallisuusajattelua kuin

muussa arkielämässä verkon ulkopuolella. Läpileikkaus hankkeen viesteissä tulee olemaan internetin ja tietoturvan maallistaminen pois sen teknisestä luonteesta. Viestit toteutetaan kohderyhmän mukaan kansantajuisesti opastaen ja turhien uhkakuvien luomista viesteissä vältetään. Lisäksi hankkeen yhtenä pitkän aikavälin tavoitteena on saada tietoturvaopetus osaksi koulujen opetussuunnitelmia.

Hankkeen tuloksena tietoturvapäivän jo hyvin toimiva konsepti paranee entisestään samalla kuin pk-sektorin erityistarpeet otetaan huomioon. Tietoturvapäivän sisällöt ja viestit leviävät laajemmin ja kohdentuvat entistä paremmin. Tietoturvatietoisuus kasvaa koko maassa.

Toteutus- ja seurantavastuu:

Päävastuu: Anna Lauttamus-Kauppila /**Viestintävirasto**
Mukana; Liikenne- ja viestintäministeriö, Keskuskauppakamari, EK, Microsoft, Suomen yrittäjät, Opetusministeriö, Opetushallitus, Sisäasiainministeriö, Kuluttajavirasto, Työ- ja elinkeinoministeriö, VTT

Aikataulu: Viestintäsuunnitelma sekä suunnitelma tietoturvapäivähankkeen kehittämisestä tulevat olla valmiit keväällä 2010.

HANKE 2: Palveluntarjoajan vastuut, oikeudet ja velvollisuudet

Tausta/ toimenpiteen sisältö:

Yhteiskunnan palvelut siirtyvät yhä voimakkaammin verkkoon, jonka tähden kansalaisten turvallinen siirtyminen palveluiden käyttäjiksi on varmistettava. Luottamuksen puute on yksi keskeisimmistä sähköisten palveluiden käyttöönoton esteistä. Kansalaisten on voitava luottaa, että verkko- ja viestintäpalveluiden käyttö on turvallista. Tässä työssä korostetaan erityisesti yhteistyön tärkeyttä ja yritysten johdon roolia ja vastuuta.

Hankkeessa selvitetään tämän hetken tilanne palveluntarjoajien vastuista, oikeuksista ja velvollisuuksista. Selvityksen pohjalta tehdään suositusluonteinen ehdotus parhaiksi käytännöiksi.

Tulos /vaikuttavuustavoite:

Hankkeen tavoitteena on lisätä palveluiden ja tuotteiden tietoturvaominaisuuksien vertailukelpoisuutta, tehdä tietoturvallisia palveluita näkyväksi sekä lisätä kansalaisten luottamusta.

Palveluntarjoajan vastuut, oikeudet ja velvollisuudet selkiintyvät ja luotettavien tietoturvaratkaisujen käyttö laajenee. Hanke edistää tietoturvan integroimista kiinteäksi osaksi tietoyhteiskunnan perusrakenteita. Yritysten valveutuneisuus tietoturva-asioista paranee.

Toteutus- ja seurantavastuu:

Päävastuu: Jaakko Turunen /**Keskuskauppakamari**
Mukana: Tietotekniikan liitto, Liikenne- ja viestintäministeriö, Oikeusministeriö, Tieto, Microsoft, Teliasonera, Kuluttajavirasto, Kesko, Valtiovarainministeriö, Työ- ja elinkeinoministeriö, Tietosuojavaltuutetun toimisto, EK, Viestintävirasto, HIIT, VTT

Aikataulu: Hanke aloittaa keväällä 2010.

3. TIETOIHIN LIITTYVIEN RISKIEN HALLINTA JA TOIMINTAVARMUUS

Toisen painopisteen toimenpiteissä tuetaan yritysten käyttöön tarkoitettujen riskienhallintamallien laajempaa käyttöönottoa, järjestetään riskienhallintaan liittyvää koulutusta. Selvitetään mitä menetelmiä ja varautumismalleja tulee kehittää entistä monimutkaisempien verkkojen ja verkostojen hallintaan, selvitetään mahdollisuutta tukea yritysten varautumis- ja riskienhallintatoimintaa, tuetaan lainsäädännöllisin keinoin yhteiskunnan elintärkeiden toimintojen tarvitsemien viestintäverkkojen ja viestintäpalvelujen toiminnan varmistamista. *

HANKE 3: Tietoihin liittyvien riskien tunnistaminen ja tietojen suojaamiseen liittyvien vaatimusten tunnistaminen (riskienhallintaa)

Tausta/ toimenpiteen sisältö:

Hankkeessa kartoitetaan tarkoituksenmukaisia riskienhallintatyökaluja ja edistetään niiden käyttöönottoa. Hankkeessa pohditaan myös miten riskienhallintaan ja palvelujen jatkuvuuteen liittyvää koulutusta voitaisiin edistää erityisesti pk-yrityksille. Lisäksi pyritään edistämään yrittäjäjärjestöjen roolia riskienhallintaan liittyvässä opastuksessa. Hankkeessa pyritään auttamaan organisaatioita selkeyttämään tietoriskien ohjausta ja hallintaa. Riskitietoisuutta lisätään tiedottamalla valikoiduista toteutuneista tietoriskeistä.

Tietojen turvallisuudesta ei kyetä enää entiseen tapaan huolehtimaan fyysisen turvallisuuden keinoin. Yritysten tulee olla perillä ajankohtaisista tietoturvallisuusvaatimuksista. Tietojen ja tietopalvelujen turvaamisen perusta syntyy erilaisien suojausvaatimusten tunnistamisesta. Vaatimuksia on asetettu mm. lainsäädännössä, sopimuksissa sekä organisaation itselleen luomissa toimintapolitiikoissa. Organisaatioissa ei välttämättä kuitenkaan osata tai pystytä tunnistamaan näitä vaatimuksia kattavasti ja systemaattisesti, mikä vaikeuttaa tavoitteellista ja tarkoituksenmukaista tietoturvallisuustyötä.

Lisäksi hankkeessa arvioidaan sellaisen menetelmän kehittämistä, jonka avulla erilaiset tietojen turvaamiseen liittyvät vaatimukset pystyttäisiin tunnistamaan ja hallitsemaan tehokkaasti. Menetelmän avulla toimijat pystyisivät kohdistamaan tietojen turvaamiseen liittyvät toimensa tehokkaammin ja tarkoituksenmukaisemmin oikeisiin asioihin.

Tulos /vaikuttavuustavoite:

Tuloksena on, että riskienhallintaosaaminen lisääntyy ja riskien ennakointi paranee. Yritysten liiketoiminnan kannalta keskeisten riskien tunnistaminen ja torjuminen vahvistuu. Riskienhallintamallien käyttöönotto lisääntyy erityisesti sellaisten yritysten keskuudessa, joilla ei ole mahdollisuutta riskienhallinnan ammattilaisten palkkaamiseen. Tietojen ja tietopalveluiden turvaaminen tulee pysyväksi osaksi yritysten riskienhallintaa.

Toteutus- ja seurantavastuu:

Päävastuu: Sauli Savisalo /**Huoltovarmuuskeskus**
Mukana: EK, Liikenne- ja viestintäministeriö, Suomen Yrittäjät, Keskuskauppakamari, Nordea, Luottokunta, VTT, FiCom, Finanssialan Keskusliitto, Keskusrikospoliisi, Puolustusministeriö, Puolustusvoimat

Aikataulu: Kartoitus aloitetaan syksyllä 2009 ja ehdotukset käyttöönoton edistämiseksi keväällä 2010

HANKE 4: Yritysten toiminnan jatkuvuuden ja kansalaisten palveluiden saatavuuden varmistaminen (toimintavarmuus)

Tausta/ toimenpiteen sisältö:

Yhteiskunnan toimintojen siirtyessä yhä suuremmassa määrin verkkoon, on tietoliikenteen häiriötön toiminta kaikissa oloissa erityisen tärkeää. Hankkeessa selvitetään, miten tieto- ja viestintäpalveluiden toimivuuden turvaamista voitaisiin edistää.

Lisäksi varautumisen ja huoltovarmuuden kannalta on olennaista selvittää vaihtoehtoiset mallit Suomen kansainvälisten tieto- ja viestintäliikenneyhteyksien turvaamiseksi mm. merikaapelissa, operaattoriyhteistyöllä, kansainvälisellä yhteistyöllä sekä satelliittiyhteyksin. Hankkeessa selvitetään mahdollisuutta rakentaa merikaapeli Suomesta Keski-Eurooppaan.

Tulos /vaikuttavuustavoite:

Tavoitteena on edistää tietoyhteiskunnan häiriönsietokykyä ja huoltovarmuutta erityisesti kasvavan viestiliikenteen tarpeisiin tulevaisuudessa. Yritysten toiminnan jatkuvuus ja kansalaisten palveluiden saatavuus tulevat paremmin varmistetuiksi. Hankkeella pyritään myös parantamaan Suomen ja suomalaisten yritysten houkuttelevuutta.

Toteutus- ja seurantavastuu:

Päävastuu: Kari Wirman /**FiCom**
Mukana: Huoltovarmuuskeskus, Liikenne- ja viestintäministeriö, Microsoft, Teliasonera, Tieto, Viestintävirasto, operaattorit, tietotekniikkatalot,

Teknologiateollisuus/tietotekniikka-ala, Tekes, Puolustusvoimat, toimihenkilöunioni, Kesko, VTT, Finanssialan keskusliitto

Aikataulu: Merikaapeli esiselvitys aloitetaan syksyllä 2009. Selvitys tietoliikennepalveluiden toimivuuden turvaamisesta valmis keväällä 2010

4. KILPAILUKYKY JA KANSAINVÄLINEN VERKOSTOYHTEISTYÖ

*Kolmannessa painopisteessä korostuu kansainvälisten standardien käyttöönoton edistäminen sekä aktiivinen osallistuminen standardien kansainväliseen kehittämistyöhön, vaikutetaan EU-yhteistyön kautta siihen, että tietoturvaan liittyvät direktiivit toimeenpannaan mahdollisimman yhdenmukaisesti, joka edistää useassa maassa toimivien suomalaisten yritysten toimintaa. Harkitaan kansallisen kv-yhteistyöverkoston perustamista, jossa tieto ja kokemukset kv-työryhmistä leviävät, selvitetään Suomen kansallisen tietoliikenneturvallisuusviranomaisen (NCSA) perustamisen tarvetta. **

HANKE 5: Suomalaisen tietoturvaosaamisen levittäminen ja aktiivinen osallistuminen standardien kansainväliseen kehittämistyöhön

Tausta/ toimenpiteen sisältö:

Suomi on useilla osa-alueilla tietoturvaosaamisen edelläkävijä, mutta sitä ei ole tarpeeksi hyvin osattu markkinoida kansainvälisesti. Suomessa ei pidä pelkästään seurata kansainvälistä kehitystä, vaan on myös pyrittävä aktiivisesti viemään maailmalle omaa tietoturvaosaamistamme. Viranomaisten ja yritysten tulisi aktiivisemmin välittää ajankohtaista tietoa muihin maihin (mm. kääntämällä uudet lait ja tärkeät säädökset englanniksi). Hankkeessa laaditaan suunnitelma Suomi-kuvan parantamiseksi tietoturvamaana.

Kansainvälisen yhteistyön avulla pystytään vaikuttamaan Suomelle oleelliseen eurooppalaisen tietoturvan kehittämiseen ja suomalaisen tietoturvatietämyksen kasvattamiseen. Hankkeessa selvitetään lisäksi miten edistetään Suomen mahdollisuuksia vaikuttaa aktiivisesti kansainvälisten standardien kehittämistyöhön sekä miten edistetään kansainvälisten standardien laajamittaista hyödyntämistä.

Tulos /vaikuttavuustavoite:

Tavoitteena on vaikuttaa yhteiseen EU politiikkaan omaehtoisen aktiivisuuden kautta ja toisaalta parantaa tiedonvaihtoa näyttämällä muille esimerkkiä. Tavoitteena on myös luoda parempia edellytyksiä kansainvälisille toimijoille tulla tai investoida Suomeen. Viranomaisten ja yritysten aktiivisuus viestiä ajankohtaisista asioista Suomen rajojen ulkopuolelle kasvaa ja Suomen maine tietoturvamaana paranee.

Kansainvälisten standardien ja parhaiden käytäntöjen noudattaminen ja siten tietoturvallinen palveluympäristö edistää Suomen kansainvälistä kilpailukykyä ja

vaikuttaa yritysten halukkuuteen investoida Suomeen. Kansallisten toimijoiden yhteistyö standardointikysymyksissä paranee.

Toteutus- ja seurantavastuu:

Päävastuu: Reijo Savola /**VTT**
Mukana: Liikenne- ja viestintäministeriö, Viestintävirasto, SFS, Nokia, Teliasonera, Teknologiateollisuus, Ulkoasiainministeriö, Sisäasiainministeriö, Tekes, Puolustusvoimat

Aikataulu: Suunnitelma valmis keväällä 2010

HANKE 6: Yritysten kilpailukyky ja NCSA

Tausta/ toimenpiteen sisältö:

Hankkeen tarkoituksena on vauhdittaa kansallisen tietoliikenne-turvallisuusviranomaisen (National Communications Security Authority, NCSA) perustamista Suomeen sekä löytää tähän tarvittava rahoitus erityisesti jatkon osalta. Virallisen NCSA:n puuttuminen vaikuttaa siten, että Suomelle luovutetaan turvaluokiteltua tietoa pidättyvästi ja toisaalta suomalaisten yritysten toimintaedellytykset kansainvälisillä markkinoilla ovat heikentyneet. Ilman NCSA:n lausuntoa suomalaiset toimijat eivät mm. voi osallistua tasavertaisesti kansainvälisiin tarjouskilpailuihin. Tietoturvallisuusviranomaistehtävien järjestämisellä on siten myös kaupallinen ja vientiteollinen intressi.

Tulos /vaikuttavuustavoite:

Suomen sisäisen ja ulkoisen turvallisuuden kannalta täysipainoinen osallistuminen turvaluokiteltua tietoa edellyttävään kansainväliseen yhteistyöhön on ensiarvoisen tärkeää. NCSA-tehtävien suorittamiseksi perustetaan riittävillä ja uskottavilla resursseilla varustettu kansallinen toimija. Kansallisen tietoliikenneturvallisuuden taso nousee Suomessa vastaamaan kehittyneeltä teollisuusvaltiolta edellytettäviä vaatimuksia sekä Suomen mahdollisuudet osallistua tasavertaisella pohjalla kansainväliseen tietoturvallisuusyhteistyöhön tulee turvatuksi.

Toteutus- ja seurantavastuu:

Päävastuu: Timo Lehtimäki /**Viestintävirasto**
Mukana: Valtiovarainministeriö, Ulkoasiainministeriö, Liikenne- ja viestintäministeriö, VTT

Aikataulu: Kansallisen tietoliikenneturvallisuusviranomaisen rahoitus jatkon osalta varmistetaan vuoden 2010 aikana

HANKE 7: Kansallisen yhteistyön tehostaminen ja aktivointi kansainvälisissä tietoturva-asioissa

Tausta/ toimenpiteen sisältö:

Suomen vähäiset resurssit kansainvälisessä vaikuttamisessa tulee suunnata tehokkaammin. Hankkeessa perustetaan kansallinen foorumi tiedonvaihdon parantamiseksi ja pohditaan myös muita toimenpiteitä kansallisen yhteistyön tehostamiseksi. Olemassa olevia hyviä kansainvälisiä foorumeita pyritään myös käyttämään aktiivisemmin vaikuttamiseen. Foorumia hyödynnetään tiedonvaihtokanavana erityisesti EU:ssa tapahtuvan tietoturvapolitiikan ja Euroopan verkko- ja viestintäviraston (ENISA) osalta.

Tulos /vaikuttavuustavoite:

Tavoitteena on tehostaa kansainvälistä yhteistyötä tarjoamalla kansallinen foorumi alan toimijoille. Tavoitteena on kokonaiskuvan parantuminen suomalaisten viranomaisten ja yksityisen sektorin edustajien kansainvälisestä toiminnasta. Tuloksena on kansallisten resurssien tehostuminen, tiedonvaihdon parantuminen sekä Suomen vaikutusmahdollisuuksien lisääntyminen.

Toteutus- ja seurantavastuu:

Päävastuu: **LVM**
Mukana: Valtiovarainministeriö, Teliasonera, Ulkoasiainministeriö, Sisäasiainministeriö, Tekes, Puolustusvoimat, Viestintävirasto

Aikataulu: Foorumin ensimmäinen tilaisuus järjestetään syksyllä 2009

5. MUUT HANKKEET

HANKE 8: Tutkimushanke lähitulevaisuuden tietoturvatrendeistä

Tausta/ toimenpiteen sisältö:

Hankkeessa kartoitetaan lähitulevaisuuden tietoturvauhkia, jotka liittyvät mm. uusiin teknologioihin, palveluihin, tuotantomalleihin ja yritysrakenteisiin. Hankkeessa pyritään identifioimaan uusia trendejä ja niihin liittyviä riskejä ja mahdollisuuksia. Kartoituksen jälkeen mahdollisia tietoturvauhkia arvioidaan erityisesti Suomen näkökulmasta. Lisäksi arvioidaan erillisen tietoturva-ohjelman perustamista.

Tulos /vaikuttavuustavoite:

Hankkeella pyritään ennakoimaan mahdollisia uusia tietoturvariskejä. Hankkeessa tuotettu tieto auttaa riskikartoitusten tekemistä eri toimialoilla. Hankkeen tavoitteena

on arvoida voidaanko tuottaa pysyvä kehityksen seurannan malli ja mekanismi, jonka avulla Suomen varautuminen tulevaisuuden haasteisiin tulee paranemaan.

Toteutus- ja seurantavastuu:

Päävastuu: Ossi Kuittinen /**SITRA**
Mukana: VTT, Tekes, Liikenne- ja viestintäministeriö, Oikeusministeriö Keskusrikospoliisi, Puolustusvoimat, Huoltovarmuuskeskus, Työ- ja elinkeinoministeriö, SUPO, Viestintävirasto, VTT

Aikataulu: Projektisuunnitelma valmis syksyllä 2009

HANKE 9: Tietoturvallisuuden mittaaminen

Tausta/ toimenpiteen sisältö:

Tietoturvallisuuden mittaaminen on sateenvarjohanke, jossa mitataan sekä strategian onnistumista että tietoturvan kehitystä yleensä. Hankkeessa selvitetään, miten tällä hetkellä tietoturvallisuuden tasoa seurataan Suomessa ja tämän pohjalta tehdään ehdotus käytettäviksi menetelmiksi ja mekanismeiksi.

Tulos /vaikuttavuustavoite:

Hankkeella varmistetaan strategian mahdollisimman tehokas toteutuminen. Lisäksi hankkeessa sovitaan indikaattorit kansallisen tietoturva-asioiden seuraamiselle. Kansallinen käsitys tietoturvan tasosta selkeytyy ja vertailukelpoisuus kansainvälisesti paranee.

Toteutus- ja seurantavastuu:

Päävastuu: Petri Puhakainen /**Oulun Yliopisto**
Mukana: Tilastokeskus, Viestintävirasto, Microsoft, Valtiovarainministeriö, VTT, Liikenne- ja viestintäministeriö, Puolustusvoimat, Tekes, Kesko, Nokia

Aikataulu: Indikaattorikartoitus on valmis keväällä 2010

6. TOIMEENPANON TOTEUTUS, SEURANTA JA RESURSSIT

Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi toimeenpannaan tällä toimenpideohjelmalla. Toimenpideohjelman jokaisessa hankkeessa on yksi organisaatio, joka on vetovastuussa kyseisestä hankkeesta (julkisen tai yksityisen sektorin taho). Strategian toteutuksen kannalta tarpeelliset toimenpiteet ja seuranta sisältyvät toimenpideohjelmaan. Tarkemmat ja yksityiskohtaisemmat toimenpiteet, mittarit ja seuranta laaditaan perustettavissa työryhmissä syksyn 2009 aikana.

Liikenne- ja viestintäministeriön asettama arjen tietoyhteiskunnan tietoturvallisuus –ryhmä tukee strategian toimeenpanon edellyttämien toimien yhteensovittamista ja seuraa strategian toteutumista. Toimenpideohjelman seuranta- ja ohjausvastuu toteutetaan siten, että hankkeiden puheenjohtajat muodostavat ”työvaliokunnan”. Valiokunta raportoi työn edistyksestä arjen tietoyhteiskunnan tietoturvallisuus –työryhmälle.

Arjen tietoyhteiskunnan tietoturvallisuus –ryhmä antaa vuosittain valtioneuvostolle kertomuksen strategian toteutumisesta ja tarpeesta päivittää strategia sekä raportoi arjen tietoyhteiskunnan neuvottelukunnalle työn etenemisestä. Valtioneuvostolla on kokonaisvastuu tietoturvastrategiasta ja se valvoo strategian toimeenpanoa sekä päivittää sitä tarpeen mukaan. Hankkeiden loppuraportit valmistuvat 28.2.2011 mennessä, jolloin arjen tietoyhteiskunnan neuvottelukunnan alaisen tietoturvallisuus –ryhmän mandaatti loppuu.

Hankkeen vetovastuussa oleva taho vastaa toimenpideohjelman toteutuksen yhteydessä syntyneistä kuluista. Toimenpideohjelma toteutetaan virkatyönä. LVM:n T&K-rahaa voi käyttää pienimuotoisiin tutkimushankkeisiin eri päätöksellä.

* (teksti suoraan valtioneuvoston periaatepäätöksestä)

"TRYGG VARDAG I INFORMATIONSSAMHÄLLET – INTE MED TUR UTAN MED KUNSKAP"

STATSRÅDETS PRINCIPEBESLUT OM EN NATIONELL INFORMATIONSSÄKERHETSSTRATEGI 4.12.2008

HANDLINGSPROGRAM

Innehåll:

1. INLEDNING

Statsrådets principbeslut on en nationell informationssäkerhetsstrategi antogs i december 2008. Syftet med strategin är att se till att finländarna kan känna sig säkra i vardagens informationssamhälle (medborgare, företag, myndigheter och andra aktörer). Den strategiska visionen är att medborgare och företag ska kunna lita på att deras information är säker både i informations- och kommunikationsnäten och i anknytande tjänster.

Medan den föregående informationssäkerhetsstrategin var gällande tog man på allvar itu med informationssäkerhetsfrågor i Finland. År 2003 offentliggjordes en informationssäkerhetsstrategi som var den första i sitt slag i Finland och Europa. Tanken med den nya strategin och det handlingsprogram som bygger på strategin är att rikta in sig på ett antal utvecklingsobjekt som experterna på området anser vara de mest centrala och få ut så konkreta resultat som möjligt från dem.

Handlingsprogrammet har beretts i en grupp för informationssäkerhet under delegationen för vardagens informationssamhälle. Uppdraget går ut på att främja informationssäkerheten i informationssamhället, bevaka informationssäkerhetens utveckling och ta initiativ till förbättringar av den. Gruppen består av fler än 20 inflytelserika aktörer inom informationssäkerheten i den offentliga och den privata sektorn. Handlingsprogrammet har lagts upp utifrån prioriteringarna i principbeslutet med syftet att nå målen i den nationella informationssäkerhetsstrategin.

Handlingsprogrammet har beretts i en så öppen process som möjligt. Programmet sammanställdes utifrån ett brett samråd om den nya informationssäkerhetsstrategin och en offentlig debatt på webbplatsen dinasikt.fi. Under beredningen har gruppen för informationssäkerhet sammanträtt fyra gånger och arrangerat ett strategiseminarium och en workshop på informationssäkerhetsdagen den 10 februari 2009. Utkastet till handlingsprogrammet sändes ut på en omfattande remiss under 2009. Inom gruppen för informationssäkerhet har det dessutom funnits ett särskilt arbetsutskott som berett handlingsprogrammet.

Den bärande tanken i handlingsprogrammet är att genomföra ett antal projekt som på ett avgörande sätt kan främja informationssäkerheten i Finland och bidra till att den nationella informationssäkerhetsstrategin blir effektivt genomförd. Meningen är att söka synergier och noga se på vilka frågor som kan ge ett mervärde. Handlingsprogrammet tangerar också andra program och de ska vägas in i arbetet (bl.a. projekt som ingår i inrikesministeriets program för den inre säkerheten). I finansministeriets strategiarbete och vid förankringen av det koncentrerar man sig på statsförvaltningens informationssäkerhet.

Utifrån strategin har 9 nyckelprojekt sammanställts i handlingsprogrammet. De ska ta upp nya aktuella informationssäkerhetsfrågor, förbättra existerande funktioner och undvika överlappningar. För varje projekt har det utsetts en projektansvarig och andra deltagare (inkluderar åtminstone de parter som nämns). De ansvariga ska se till att det tas fram indikatorer att följa upp projekten med. Gruppen för informationssäkerhet i vardagens informationssamhälle har ansvar för att samordna handlingsprogrammet.

2. BASKUNSKAPER I VARDAGENS INFORMATIONSSAMHÄLLE

Den första prioriteringen omfattar insatser för att utveckla projektet för en nationell informationssäkerhetsdag, öka människors medvetenhet om informationssäkerhet, följa upp medvetenhetsnivån, förbättra kunnandet i informationssäkerhet och göra upp en aktiv och framsynt kommunikationsplan. Målet är att komplettera varje anbudsbegäran med krav på informationssäkerhet, inkl. planeringsfaserna av lösningarna och tjänsterna, arbeta för att införa informationssäkerhetslösningar på bredare front, utreda möjligheten att utveckla ett särskilt certifikat för säkra tjänster och främja en ökning av antalet certifierade sakkunniga specialiserade på informationssäkerhet i Finland.*

PROJEKT 1: Ökad medvetenhet om informationssäkerhet

Bakgrund/insats:

För att informationssamhället ska fungera måste det tillhandahålla garanterat säkra tjänster. Alla som medverkar i informationssamhället har ett ansvar för informationssäkerheten och alla parter måste inse sin andel i ansvaret. Därför är det särskilt viktigt att hela samhället uppfostras till insikt om informationssäkerhet.

Projektet bedömer vad som menas med baskunskaper i informationssäkerhet i vardagens informationssamhälle och utifrån detta utarbetas meddelanden om informationssäkerhet för alla centrala befolkningsgrupper. En särskild kommunikationsplan utarbetas för att gå ut med informationen.

Projektet utvärderar behoven av att utveckla konceptet för Informationssäkerhetsdagen, varav det främsta är att utvidga dagen till att omfatta hela landet. Ambitionen är att kunna ordna en informationssäkerhetsdag regionalt och lokalt, inte bara i huvudstadsregionen. Informationssäkerhetsdagen ordnas varje år i februari och den är ett gemensamt projekt för den offentliga förvaltningen, näringslivet och organisationerna. Syftet är att öka medborgarnas medvetenhet om informationssäkerhet.

Projektet noterar särskilt sektorn för små och medelstora företag (sm-sektorn), så att man utreder möjligheterna att skapa ett eget informationssäkerhetsprojekt för den sektorn. I kommunikationen om informationssäkerhet till den här sektorn ska företagens behov prioriteras framom tekniska aspekter. Meddelanden om informationssäkerheten ska bli en integrerad del av företagens affärsverksamhet.

Det finska skolsystemet utgör grunden för den nationella kompetensen inom informationssäkerhet. Det ska ses till att alla skolelever och studerande får utbildning i informationssäkerhet och den ska utvidgas också utanför datautbildningen. Projektet ska bidra till att färdigheterna för informationssäkerhet utvecklas på alla utbildningsstadier.

Resultat/önskad effekt:

Det allmänna målet är att medvetenheten om informationssäkerhet nationellt ska bli bättre och ansvar, rättigheter och skyldigheter kring informationssäkerhet tydligare. Informationssamhället har gjort det möjligt att sköta en mängd olika dagliga sysslor och funktioner på nätet och därför ska man där tillämpa samma regler och säkerhetstänkande som i det dagliga livet utanför nätet. Projektmeddelandena kommer i snitt att gå ut på att förankra Internet och informationssäkerheten i verkligheten och tona ner den tekniska aspekten. Informationen förmedlas med hänsyn till respektive målgrupp genom användartillvänd handledning och onödiga hotbilder ska undvikas. Ett av projektets långsiktiga mål är att integrera utbildningen i informationssäkerhet i skolornas läroplaner.

Som resultat av projektet förbättras det redan välfungerande konceptet för informationssäkerhetsdagen samtidigt som sm-sektorns särskilda behov beaktas. Informationssäkerhetsdagens innehåll och budskap sprids i allt vidare kretsar och med allt bättre fokusering. Medvetenheten om informationssäkerheten ökar i hela landet.

Ansvar för genomförande och uppföljning:

Huvudansvarig: Anna Lauttamus-Kauppila/**Kommunikationsverket**

Medverkande: kommunikationsministeriet, Centralhandelskammaren, Finlands Näringsliv, Microsoft, Företagarna i Finland, undervisningsministeriet, Utbildningsstyrelsen, inrikesministeriet, Konsumentverket, arbets- och näringsministeriet, VTT

Tidsplan: Kommunikationsplanen och planen för utveckling av projektet för informationssäkerhetsdagen ska vara färdiga våren 2010.

PROJEKT 2: Tjänsteleverantörens ansvar, rättigheter och skyldigheter

Bakgrund/insatser:

Samhällets tjänster flyttas i allt större utsträckning över på nätet och då måste det ses till att det är säkert för medborgarna att anlita nättjänster. Bristande förtroende är ett av de största hindren för införandet av e-tjänster. Medborgarna måste kunna lita på att det är säkert att använda nät- och kommunikationstjänster. I det här arbetet är samverkan och företagsledningens roll och ansvar särskilt viktiga.

Projektet ska utreda hur tjänsteleverantörernas ansvar, rättigheter och skyldigheter ser ut just nu. Utredningen ska utmynna i ett förslag om bästa praxis som har karaktären av rekommendation.

Resultat/önskad effekt:

Projektet avser att förbättra jämförbarheten mellan tjänsters och produkters informationssäkerhetsegenskaper, synliggöra informationssäkerhetstjänsterna och öka medborgarnas förtroende.

Tjänsteleverantörens ansvar, rättigheter och skyldigheter förtydligas och användningen av tillförlitliga informationssäkerhetslösningar ökar. Projektet främjar en integrering av informationssäkerheten i informationssamhällets grundstrukturer. Företagens insikter i informationssäkerhetsfrågor förbättras.

Ansvar för genomförande och uppföljning:

Huvudansvarig: Jaakko Turunen/**Centralhandelskammaren**

Medverkande: Tietotekniikan Liitto, kommunikationsministeriet, justitieministeriet, Tieto, Microsoft, Teliasonera, Konsumentverket, Kesko, finansministeriet, arbets- och näringsministeriet, dataombudsmannens byrå, Finlands Näringsliv, Kommunikationsverket, Forskningsinstitutet för Informationsteknologi HIIT, VTT

Tidsplan: Projektet inleds våren 2010.

3. HANTERING AV INFORMATIONSRISKERNA OCH FUNKTIONSSÄKERHET

Den andra prioriteringen omfattar insatser för att stödja företagen i att införa företagsspecifika riskhanteringsmodeller i större skala och att ordna utbildning om riskhantering. Det ska utredas vilka metoder och beredskapsmodeller som bör tas fram för att hantera allt mer komplicerade nät och nätverk, hur företagen kan stödjas i sin beredskap och riskhantering och hur kommunikationsnät och kommunikationstjänster som är nödvändiga för samhällsviktiga funktioner kan säkerställas genom lagstiftningsåtgärder.

PROJEKT 3: Hur man identifierar informationsriskerna och dataskyddskraven (riskhantering)

Bakgrund/insatser:

Projektet ska kartlägga lämpliga riskhanteringsverktyg och främja deras användning. Projektet ska också överväga hur utbildningen i riskhantering och tjänstekontinuitet kan främjas framför allt för sm-företag. Företagarorganisationernas roll i handledningen i riskhantering ska stödjas. Ambitionen är att hjälpa organisationer att styra och hantera informationsriskerna. Riskmedvetenheten främjas dessutom genom att man selektivt offentliggör informationsrisker som realiserats.

Det går inte längre att tillgodose informationssäkerheten med fysiska säkerhetsmetoder. Företagen bör vara insatta i aktuella informationssäkerhetskrav. Grunden för säker information och säkra informationstjänster är att man identifierar olika slag av informationssäkerhetskrav. Kraven bygger bl.a. på lagstiftning, avtal och organisationernas egna policyer. Men det är inte självklart att organisationer går i land med att identifiera kraven fullt ut och systematiskt och det försvårar i sin tur ett målinriktat och ändamålsenligt informationssäkerhetsarbete.

Projektet ska också utvärdera om det går att ta fram en metod som kan hjälpa till att identifiera och hantera olika informationssäkerhetskrav på ett effektivt sätt. Metoden ska hjälpa aktörer att rikta in sina informationssäkerhetsinsatser på de rätta frågorna på ett effektivare och ändamålsenligare sätt.

Resultat/önskad effekt:

Resultatet är att riskhanteringskompetensen ökar och att det blir lättare att förutse risker. Företagen blir bättre på att identifiera och avvärja centrala risker för sin verksamhet. Riskhanteringsmodeller införs i större omfattning inte minst i företag som inte har någon möjlighet att anställa en fackman på riskhantering. Att säkra information och informationstjänster blir ett bestående inslag i företagens riskhantering.

Ansvar för genomförande och uppföljning:

Huvudansvarig: Sauli Savisalo/**Försörjningsberedskapscentralen**

Medverkande: Finlands Näringsliv, kommunikationsministeriet, Företagarna i Finland, Centralhandelskammaren, Nordea, Kreditlaget, VTT, FiCom, Finansbranschens centralförbund, Centralkriminalpolisen, försvarsministeriet, försvarsmakten

Tidsplan: Kartläggningen inleds hösten 2009 och förslagen om införande våren 2010.

PROJEKT 4: Hur man säkerställer kontinuiteten i företagens verksamhet och medborgarnas tillgång till tjänster (funktionssäkerhet)

Bakgrund/insats:

Samhällets funktioner flyttas i allt större utsträckning över på nätet och då är det speciellt viktigt att kommunikationerna fungerar störningsfritt. Projektet klarlägger hur man kan säkra att informations- och kommunikationstjänsterna fungerar.

Dessutom är det för beredskapen och försörjningsberedskapen väsentligt att man klarlägger alternativen för att säkra Finlands internationella informations- och kommunikationsförbindelser bl.a. per havskabel, genom operatörssamarbete, internationellt samarbete och satellitförbindelser. Projektet ska utreda om det går att dra en havskabel från Finland till Mellaneuropa.

Resultat/önskad effekt:

Syftet är att främja informationssamhällets förmåga att hantera störningar och försörjningsberedskap framför allt med tanke på framtidens ökande kommunikationer. Det ska bli lättare att säkra kontinuiteten i företagens verksamhet och medborgarnas tillgång till tjänster. Projektet ska också göra Finland och finska företag mer attraktiva.

Ansvar för genomförande och uppföljning:

Huvudansvarig: Kari Wirman/**FiCom**

Medverkande: Försörjningsberedskapscentralen, kommunikationsministeriet, Microsoft, Teliasonera, Tieto, Kommunikationsverket, operatörer, datateknikföretag Teknologiindustrin/informationstekniksektorn, Tekes, försvarsmakten, Tjänstemannaunionen, Kesko, VTT, Finansbranschens Centralförbund

Tidsplan: En förberedande utredning om en havskabel ska vara färdig hösten 2009. Utredningen om hur informationstjänsternas funktion säkras ska vara färdig våren 2010.

4. KONKURRENSKRAFT OCH INTERNATIONELLT NÄTVERKSSAMARBETE

Den tredje prioriteringen lyfter fram insatser för att införa internationella standarder, att delta aktivt i den internationella utvecklingen av standarder och att utnyttja EU-samarbetet för att påverka att direktiven om informationssäkerhet genomförs så samordnat som möjligt, vilket gynnar finska företag som är verksamma i flera länder. Ett nationellt nätverk för internationellt samarbete för att sprida kunskap och erfarenheter från internationella arbetsgrupper ska övervägas och det ska klarläggas om det finns behov av att inrätta en nationell myndighet för informationssäkerhet (NCSA) i Finland.*

PROJEKT 5: Hur man sprider finländskt kunnande om informationssäkerhet och aktivt deltar i det internationella arbetet med att ta fram standarder

Bakgrund/insats:

Finland ligger i utvecklingens framkant på flera delområden av informationssäkerhet, men man har varit dålig på att marknadsföra den kompetensen. Vi bör inte bara bevaka den internationella utvecklingen utan också aktivt försöka gå ut i världen med vårt kunnande på området. Myndigheter och företag bör visa större aktivitet i att förmedla aktuell information till andra länder (bl.a. genom att låta översätta nya lagar och viktiga författningar till engelska). Projektet ska lägga upp en plan för hur bilden av Finland som ett land som satsar på informationssäkerhet ska synliggöras.

Genom internationellt samarbete kan vi påverka utvecklingen av den för oss så viktiga europeiska informationssäkerheten och öka kunskapen om finsk informationssäkerhet. Projektet ska klarlägga Finlands möjligheter att aktivt påverka den internationella utvecklingen av standarder och hur internationella standarder ska utnyttjas i stor skala.

Resultat/önskad effekt:

Ambitionen är att påverka den gemensamma politiken i EU genom egen aktivitet och förbättra informationsutbytet genom att föregå med gott exempel. Vidare är syftet att underlätta för internationella aktörer att etablera sig eller investera i Finland. Myndigheter och företag ska bli bättre på att informera om aktuella frågor utanför Finlands gränser och Finlands rykte som ett land som satsar på informationssäkerhet förbättras.

Finlands internationella konkurrenskraft och företagens intresse för att investera i Finland främjas bäst av att vi följer internationella standarder och bästa praxis och därmed garanterar en säker

omvärld för informationstjänsterna. Nationella aktörers samarbete i standardiseringsfrågor ska bli bättre.

Ansvar för genomförande och uppföljning:

Huvudansvarig: Reijo Savola/**VTT**

Medverkande: kommunikationsministeriet, Kommunikationsverket, Finlands Standardiseringsförbud SFS, Nokia, Teliasonera, Teknologiindustrin, utrikesministeriet, inrikesministeriet, Tekes, försvarsmakten

Tidsplan: Planen ska vara färdig våren 2010.

PROJEKT 6: Företagens konkurrenskraft och NCSA

Bakgrund/insatser:

Projektet har till uppgift att påskynda en nationell myndighet för informationssäkerhet (National Communications Security Authority, NCSA) i Finland och ordna med nödvändig finansiering för fortsättningen. Eftersom Finland saknar en nationell myndighet, överlämnas säkerhetsklassificerad information till Finland med stor återhållsamhet och finska företags verksamhetsvillkor på den internationella marknaden försvagas därmed. Utan utlåtande från NCSA kan finska aktörer t.ex. inte delta på lika villkor i internationella anbudstävlingar. Handeln och exportindustrin har alltså också ett intresse av att en myndighet för informationssäkerhet inrättas.

Resultat/önskad effekt:

För Finlands yttre och inre säkerhet är det utomordentligt viktigt att vi kan delta fullt ut i internationellt samarbete som kräver säkerhetsklassificerad information. För NCSA-uppgifter inrättas en nationell aktör som förses med tillräckliga och trovärdiga resurser. Nivån på den nationella informationssäkerheten stiger i Finland till en nivå som anstår ett utvecklat industriland och Finlands möjligheter att delta på lika villkor i det internationella samarbetet om informationssäkerhet förbättras.

Ansvar för genomförande och uppföljning:

Huvudansvarig: Timo Lehtimäki/**Kommunikationsverket**

Medverkande: finansministeriet, utrikesministeriet, kommunikationsministeriet, VTT

Tidsplan: Fortsatt finansiering av en nationell myndighet för informationssäkerhet säkras under 2010.

PROJEKT 7: Ett effektivare nationellt samarbete och aktivare insatser i internationella informationssäkerhetsfrågor

Bakgrund/insatser:

Finlands knappa resurser för internationell medverkan bör riktas effektivare. Genom projektet inrättas ett nationellt forum för bättre informationsutbyte och planeras andra insatser för att förbättra det nationella samarbetet. Existerande lämpliga internationella fora utnyttjas mer aktivt för påverkan. Det nationella forumet nyttiggörs som kanal för informationsutbyte främst i fråga om informationssäkerhetspolitiken inom EU och Europeiska byrån för nät- och informationssäkerhet (ENISA).

Resultat/önskad effekt:

Ambitionen är att göra det internationella samarbetet effektivare genom att erbjuda aktörer på området ett nationellt forum. Målet är att förbättra den allmänna uppfattningen om finska myndigheters och privat sektors internationella aktiviteter. Det ska resultera i effektivare användning av nationella resurser, bättre informationsutbyte och ökat medinflytande för Finland.

Ansvar för genomförande och uppföljning:

Huvudansvarig: kommunikationsministeriet

Medverkande: finansministeriet, Teliasonera, utrikesministeriet, inrikesministeriet, Tekes, försvarsmakten, Kommunikationsverket

Tidsplan: Forumet ordnar sin första tillställning hösten 2009

5. ÖVRIGA PROJEKT

PROJEKT 8: Forskningsprojekt om trenderna inom informationssäkerheten i den närmaste framtiden

Bakgrund/insats:

Projektet ska kartlägga sådana hot mot informationssäkerheten i den närmaste framtiden som har samband med bl.a. ny teknik, tjänster, produktionsmodeller och företagsstrukturer. Meningen är att identifiera nya trender samt riskerna och möjligheterna kring dem. Efter kartläggningen ska eventuella hot mot informationssäkerheten bedömas särskilt ur finländsk synvinkel. Dessutom ska frågan om ett särskilt program för informationssäkerhet tas upp till bedömning.

Resultat/önskad effekt:

Projektet ska förutse eventuella nya informationssäkerhetsrisker. Informationen underlättar en kartläggning av riskerna i de olika sektorerna. Ambitionen är att ta fram en bestående modell och mekanism för uppföljning av utvecklingen för att ge Finland bättre möjligheter att förbereda sig för framtidens utmaningar.

Ansvar för genomförande och uppföljning:

Huvudansvarig: Ossi Kuittinen/**SITRA**

Medverkande: VTT, Tekes, kommunikationsministeriet, justitieministeriet, Centralkriminalpolisen, försvarsmakten, Försörjningsberedskapscentralen, arbets- och näringsministeriet, skyddspolisen, Kommunikationsverket

Tidsplan: Projektplanen är färdig hösten 2010.

PROJEKT 9: Hur man mäter informationssäkerheten

Bakgrund/insatser:

Mätningen av informationssäkerheten är ett paraplyprojekt som mäter dels hur strategin slagit i genom, dels hur informationssäkerheten utvecklats över lag. Projektet ska klarlägga hur nivån på informationssäkerheten följs upp i Finland i dag och utifrån detta läggs förslag om de metoder och mekanismer som ska användas.

Resultat/önskad effekt:

Projektet ska säkerställa att strategin genomförs så effektivt som möjligt. Dessutom ska man komma överens om vilka indikatorer som används för att följa upp informationssäkerhetsfrågor nationellt. Den nationella uppfattningen om nivån på informationssäkerheten klarnar och jämförbarheten internationellt förbättras.

Ansvar för genomförande och uppföljning:

Huvudansvarig: Petri Puhakainen/**Uleåborgs universitet**

Medverkande: Statistikcentralen, Kommunikationsverket, Microsoft, finansministeriet, VTT, kommunikationsministeriet, försvarsmakten, Tekes, Kesko, Nokia

Tidsplan: Kartläggningen av indikatorer ska vara klar våren 2010

6. GENOMFÖRANDE, UPPFÖLJNING OCH RESURSER

Statsrådets principbeslut om en strategi för informationssäkerhet ska genomföras med detta handlingsprogram. För varje projekt i handlingsprogrammet anges en organisation med ansvar för projektet (inom den offentliga eller privata sektorn). I programmet anges vidare de insatser och den uppföljning som behövs för att genomföra strategin. Närmare och mer detaljerade insatser, indikatorer och uppföljningsåtgärder läggs upp av de arbetsgrupper som tillsätts hösten 2009.

Den arbetsgrupp för informationssäkerhet inom vardagens informationssamhälle som tillsatts av kommunikationsministeriet hjälper till att samordna de insatser som behövs för att genomföra strategin och följer upp den. Ansvaret för uppföljning och styrning av handlingsprogrammet

fullföljs så att projektordförandena bildar ett ”arbetsutskott”. Utskottet rapporterar till arbetsgruppen ovan hur arbetet fortskrider.

Arbetsgruppen lämnar årligen en berättelse till statsrådet om hur strategin har realiserats och huruvida den behöver uppdateras och rapporterar till delegationen för vardagens informationssamhälle om framstegen. Statsrådet har det samlade ansvaret för strategin för informationssäkerhet och det bevakar genomförandet och uppdaterar strategin efter behov. Projekten ska ha sina slutrapporter färdiga senast den 28 februari 2011, då arbetsgruppens mandattid löper ut.

Den projektansvariga parten svarar för kostnaderna för genomförande av handlingsprogrammet. Programmet genomförs som tjänsteuppdrag. Kommunikationsministeriets anslag för forskning och utveckling kan genom särskilt beslut användas för småskaliga forskningsprojekt.

- (texten är hämtad ur statsrådets principbeslut)

"EVERYDAY SECURITY IN THE INFORMATION SOCIETY – A MATTER OF SKILLS, NOT OF LUCK"

THE GOVERNMENT RESOLUTION ON
NATIONAL INFORMATION SECURITY STRATEGY
4 DECEMBER 2008

ACTION PROGRAMME

Contents:

1. INTRODUCTION

The Government Resolution on National Information Security Strategy was approved in December 2008. The aim of the National Information Security Strategy is to make everyday life in the information society safe and secure for everyone in Finland (individuals, businesses, administrative authorities and other actors). The strategy's vision is that individuals and businesses will be able to trust in the security of their data on information and communication networks and in related services.

During the previous information security strategy, information security work was carried out in Finland on a broad front. The information security strategy published in 2003 was the first of its kind in Finland and Europe. The aim of the new strategy and the action programme based on it is to focus on a few projects considered to be important by experts in the field and to achieve concrete results through them.

The action programme has been prepared by the Information Security Group, which works under the Ubiquitous Information Society Advisory Board. The group's task is to promote information security in the information society, monitor progress in the development of information security and to make initiatives to improve information security. The group comprises more than 20 players from the public and private sectors. The action programme has been prepared, based on the priorities of the Government Resolution, to achieve the objectives of the National Information Security Strategy.

In preparing the action programme, the aim has been to keep the process as open as possible. An extensive consultation round on the new information security strategy was held as the basis for formulating the action programme, and public debate on the issue was initiated on the website otakantaa.fi. During preparation of the action programme, the Information Security Group convened four times and arranged a strategy seminar and workshop on Information Security Day on 10 February 2009. A draft of the action programme was extensively circulated for consultation during 2009. Moreover, a separate working group preparing the action programme has operated within the Information Security Group.

A key idea of the action programme is that it will execute several key projects that will decisively promote information security in Finland and thus effectively implement the National Information Security Strategy. The intention is to seek synergies and consider precisely in which areas added value can be generated. The action programme also has interfaces with other programmes, which will be taken into account in the work (e.g. certain projects belonging to the Ministry of the Interior's internal security programme). The Ministry of Finance's strategy work focuses on the information security of public administration.

Based on the strategy, the action programme brings together nine key projects, which will address new topical information security issues, improve existing work and avoid overlapping measures. A leader and other participants (including the above-mentioned parties) have been appointed for each project. Under the direction of those in positions of responsibility, indicators will be created for the projects to aid in monitoring their implementation. The Ubiquitous Information Society Information Security Group has coordinating responsibility for the action programme.

2. BASIC SKILLS IN THE UBIQUITOUS INFORMATION SOCIETY

The measures of the first priority will develop the National Information Security Day project, improve information security awareness, monitor the level of awareness, develop information security skills and prepare a proactive communications plan. Information security requirements will be increased as part of every invitation to tender, including the planning phases of solutions and services; more extensive use of information security solutions will be promoted; the possibility of introducing special certification for security services will be investigated; an increase in the number of certified information security professionals in Finland will be promoted.

PROJECT 1: Increasing information security awareness

Background/content of the measure:

A requirement of an efficient information society is that the security of the services it provides can be safeguarded. Information security is the responsibility of all those who participate in the information society and everyone must understand their share of this division of responsibility. Because of this it is particularly important to improve understanding of information security everywhere in society.

The project will assess what basic skills in the ubiquitous information society mean and, based on this, will prepare information security communications for all the main population groups. A separate communications plan will be prepared for the dissemination of these messages.

The project will also assess the development needs of the Information Security Day concept, the most important of which is expanding the Information Security Day to cover the whole of Finland. The Information Security Day project will aim to arrange Information Security Day events not only in the Helsinki Metropolitan Area but also on regional and local levels. The Information Security Day, which is held annually in February, is a joint project of the public administration, businesses and organisations, and its purpose is to improve the information security awareness of the public.

The project will particularly take into account the SME sector, such that opportunities to create a specific information security project for the SME sector are investigated. Information security communications directed at SMEs will take into account better than at present the needs of businesses instead of emphasising technical aspects. Information security communications will be closely incorporated into companies' business outlook.

The Finnish school system is the foundation for national information security competence. Information security education will be safeguarded for all pupils and students and it should also be expanded outside the sphere of IT education. The project will aim to encourage the development of information security preparedness at all levels of education.

Performance/effectiveness target:

The general goal is to improve national information security awareness and to clarify information security responsibilities, rights and obligations. The information society has enabled many everyday tasks and actions to be handled comprehensively on the internet, so the same rules and security philosophy should be followed there as in other areas of everyday life outside the internet. The orientation of the project's communications will be to make the internet and information security more familiar, with less focus on their technical aspects. According to the target group, communications will be instructive in a commonsense way, avoiding messages that generate unnecessary threats. Moreover, one long-term objective of the project is to make information security education part of the school curriculum.

As a result of the project, the already highly effective Information Security Day concept will be further improved taking into account the special needs of the SME sector. The Information Security Day's content and messages will be disseminated more widely and targeted better. Information security awareness will grow throughout the whole of Finland.

Implementation and monitoring responsibility:

Main responsibility: Anna Lauttamus-Kauppila /**Finnish Communications Regulatory Authority**
Participating: Ministry of Transport and Communications, Central Chamber of Commerce, Confederation of Finnish Industries EK, Microsoft, Federation of Finnish Enterprises, Ministry of Education, National Board of Education, Ministry of the Interior, Finnish Consumer Agency, Ministry of Employment and the Economy, Technical Research Centre of Finland VTT.

Timetable: A communications plan and a plan for the development of the Information Security Day project will be ready in spring 2010.

PROJECT 2: Service provider's responsibilities, rights and obligations

Background/content of the measure:

Society's services are increasingly being transferred on to the internet, and as a result the secure transition of the public to become users of services must be ensured. A lack of trust is one of the main barriers to the introduction of electronic services. The public must be able to trust that their use of internet and communications services is secure. This work will highlight in particular the importance of cooperation and the roles and responsibilities of company management.

The project will review the current situation in terms of service providers' responsibilities, rights and obligations. Based on the study, a recommendation on best practices will be proposed.

Performance/effectiveness target:

The objective of the project is to improve comparability of the information security features of services and products, to make information security services more visible, and to increase the public's trust in electronic services.

The service provider's responsibilities, rights and obligations will be clarified and the use of reliable information security solutions expanded. The project will promote the close integration of information security into the basic structures of the information society. Companies' awareness of information security will improve.

Implementation and monitoring responsibility:

Main responsibility: Jaakko Turunen /**The Central Chamber of Commerce**
Participating: Finnish Information Processing Association, Ministry of Transport and Communications, Ministry of Justice, Tieto, Microsoft, Teliasonera, Finnish Consumer Agency, Kesko, Ministry of Finance, Ministry of Employment and the Economy, Office of the Data Protection Ombudsman, Confederation of Finnish Industries EK, Finnish Communications Regulatory Authority, Helsinki Institute for Information Technology HIIT, Technical Research Centre of Finland VTT.

Timetable: The project will begin in spring 2010.

3. INFORMATION RISK MANAGEMENT AND PROCESS RELIABILITY

The measures of the second priority will provide support for the wider adoption of risk management models for business and arrange risk management training. Research will be carried out on how procedures and response capabilities should be developed for ever more complex networks and network administration; opportunities to support preparedness and risk management in business will be explored; legislative support will be provided to safeguard the communication networks and services for functions vital to society.

PROJECT 3: Identifying information risks and data protection requirements (risk management)

Background/content of the measure:

The project will survey appropriate risk management tools and promote their adoption. The project will also consider how training related to risk management and service continuity can be promoted, particularly in SMEs. Moreover, the aim is to promote the role of business organisations in risk management guidance and information. A further objective of the project is to help organisations clarify the supervision and management of their information risks. Risk awareness will be enhanced by publicising selected examples of real and actual information risks.

It is no longer possible, as it once was, to attend to information security by means of physical security. Companies must be fully aware of current information security requirements. The security of information and information services is based on the identification of various protection requirements. These requirements have been laid down, for example, in legislation, agreements and in operating policies created by organisations themselves. Organisations are not necessarily able, however, to identify these requirements comprehensively and systematically, which adversely affects target-driven and appropriate information security work.

In addition, the project will assess the development of a method to aid the identification and control of various information security requirements. Using the method, actors would be able to target their information security measures more effectively and appropriately at the right issues.

Performance/effectiveness target:

The outcome will be a boost to risk management expertise and an improvement in risk forecasting. Identification and prevention of the main risks for business operations will be strengthened. The adoption of risk management models will be increased, particularly among companies which have no possibility of hiring risk management professionals. Information and information services security will become a permanent part of companies' risk management.

Implementation and monitoring responsibility:

Main responsibility: Sauli Savisalo /**National Emergency Supply Agency**
Participating: Confederation of Finnish Industries EK, Ministry of Transport and Communications, Federation of Finnish Enterprises, Central Chamber of Commerce, Nordea, Luottokunta, Technical Research Centre of Finland VTT, Finnish Federation for Communications and Teleinformatics FiCom, Federation of Finnish Financial Services, National Bureau of Investigation, Ministry of Defence, Defence Forces.

Timetable: The survey will begin in autumn 2009 and proposals to promote adoption will be announced in spring 2010.

PROJECT 4: Safeguarding continuity of business activities and the public's access to services (reliability)

Background/content of the measure:

As society's functions are increasingly transferred to the internet, trouble-free operation of telecommunications is particularly important under all circumstances. The project will review the means by which the functionality of information and communications services can be safeguarded.

Moreover, in terms of contingency and national security of supply, it is essential to review alternative models to safeguard Finland's international information and communications links, for example, in undersea cables, operator cooperation,

international cooperation and satellite links. The project will investigate the possibility of building an undersea cable from Finland to Central Europe.

Performance/effectiveness target:

The objective is to promote the robustness and security of supply of the information society, particularly for the needs of growing communications traffic. Continuity of business activities and the public's access to services will be better safeguarded. The aim of the project is also to improve the attractiveness of Finland and Finnish companies.

Implementation and monitoring responsibility:

Main responsibility: Kari Wirman / **Finnish Federation of Communications and Teleinformatics FiCom**
Participating: National Emergency Supply Agency, Ministry of Transport and Communications, Microsoft, Teliasonera, Tieto, Finnish Communications Regulatory Authority, operators, information technology companies, Federation of Finnish Technology Industries/information technology sector, Finnish Funding Agency for Technology and Innovation TEKES, Defence Forces, Union of Salaried Employees, Kesko, Technical Research Centre of Finland VTT, Federation of Finnish Financial Services.

Timetable: A preliminary study on an undersea cable will begin in autumn 2009. A study on safeguarding the functionality of telecommunication services will be ready in spring 2010.

4. COMPETITIVENESS AND INTERNATIONAL NETWORK COOPERATION

The third priority emphasises promoting the adoption of international standards and active participation in international development work as well as active involvement in EU cooperation to ensure that information security directives are implemented in as uniform a way as possible, thus promoting the activities of Finnish companies operating in several countries. The creation of a national network for the purposes of exchanging information and experiences of international working groups will be considered, and the need to establish a National Communications Security Authority (NCSA) will be examined.

PROJECT 5: Promoting Finnish information security expertise and active participation in international standards development work

Background/content of the measure:

Finland is a pioneer of information security expertise in many areas, but it has made limited progress in marketing this expertise internationally. Finland should not merely follow international development; it must also make active efforts to export its own

information security expertise. Administrative authorities and companies should convey topical information more actively to other countries (for example by translating new laws and important statutes into English). The project will prepare a plan to improve the image of Finland as an information security country.

International cooperation will help develop European information security, which is essential for Finland, and improve Finnish knowledge of information security. The project will also investigate how to promote Finland's opportunities to actively influence international standards development work and how to promote the widescale utilisation of international standards.

Performance/effectiveness target:

The objective is to influence joint EU policy via independent activity and, furthermore, to improve exchange of information by showing an example to others. A further aim is to create better conditions for international actors to come to or invest in Finland. The activity of authorities and companies in communicating topical issues outside Finland's borders will grow and Finland's reputation as an information security company will improve.

Adhering to international standards and best practices and therefore a secure service environment will promote Finland's international competitiveness and affect companies' willingness to invest in Finland. Cooperation with national actors on standardisation issues will improve.

Implementation and monitoring responsibility:

Main responsibility: Reijo Savola /**The Technical Research Centre of Finland VTT**
Participating: Ministry of Transport and Communications, Finnish Communications Regulatory Authority, Finnish Standards Association SFS, Nokia, Teliasonera, Federation of Finnish Technology Industries, Ministry for Foreign Affairs, Ministry of the Interior, Finnish Funding Agency for Technology and Innovation TEKES, Defence Forces.

Timetable: Plan ready in spring 2010.

PROJECT 6: Business competitiveness and the NCSA

Background/content of the measure:

The project's purpose is to accelerate the establishment in Finland of a National Communications Security Authority (NCSA) and to find the necessary funding for this, particularly in terms of the future. The lack of an official NCSA has contributed to the fact that security classified information has been transferred to Finland only modestly and, moreover, Finnish companies' operating conditions in international markets have been weakened. Without an NCSA opinion, Finnish actors cannot, for example, participate on an equal basis in international competitive tenders. There is therefore also a commercial and export-industry dimension to the arrangement of information security official tasks.

Performance/effectiveness target:

In terms of Finland's internal and external security, full participation in international cooperation requiring security-classified information is of prime importance. A national actor with sufficient and credible resources will be established to perform NCSA tasks. National telecommunications security will be raised in Finland to the level required of an advanced industrial country, and Finland's opportunities to participate on an equal basis in international information security cooperation will be safeguarded.

Implementation and monitoring responsibility:

Main responsibility: Timo Lehtimäki /**The Finnish Communications Regulatory Authority**
Participating: Ministry of Finance, Ministry for Foreign Affairs, Ministry of Transport and Communications, Technical Research Centre of Finland VTT.

Timetable: The funding of the National Communications Security Authority in terms of the future will be confirmed during 2010.

PROJECT 7: Enhancing and activating national cooperation in international information security issues

Background/content of the measure:

Finland's modest resources in terms of international influence should be directed more effectively. The project will establish a national forum to improve exchange of information and will also consider other measures to enhance national cooperation. The aim is also to utilise existing good international forums more actively. The national forum will be utilised as a channel for information exchange particularly with respect to EU information security policy and the European Network and Information Security Agency (ENISA).

Performance/effectiveness target:

The objective is to enhance international cooperation by providing a national forum for sector actors. A further aim is to improve the overall situation in terms of the international activity of Finnish administrative authorities and private sector representatives. The result will be more effective use of national resources, an improvement in information exchange, and increased opportunities for Finland to influence issues.

Implementation and monitoring responsibility:

Main responsibility: **The Ministry of Transport and Communications**

Participating: Ministry of Finance, Teliasonera, Ministry for Foreign Affairs, Ministry of the Interior, Finnish Funding Agency for Technology and Innovation TEKES, Defence Forces, Finnish Communications Regulatory Authority.

Timetable: The forum's first event will be held in autumn 2009.

5. OTHER PROJECTS

PROJECT 8: Research project on near-future information security trends

Background/content of the measure:

The project will survey near-future information security threats, which relate for example to new technologies, services, production models and corporate structures. The project will endeavour to identify new trends as well as the risks and opportunities related to them. Following the survey, possible information security threats will be assessed, particularly from the perspective of Finland. In addition, an assessment will be made of the establishment of a separate information security programme.

Performance/effectiveness target:

The objective of the project is to anticipate possible new information security risks. Information generated in the project will aid the making of risk surveys in different sectors. A further aim of the project is to assess whether it is possible to produce a permanent development-monitoring model, which will help improve Finland's preparations for future challenges.

Implementation and monitoring responsibility:

Main responsibility: Ossi Kuittinen /**The Finnish Innovation Fund SITRA**
Participating: Technical Research Centre of Finland VTT, Finnish Funding Agency for Technology and Innovation TEKES, Ministry of Transport and Communications, Ministry of Justice, National Bureau of Investigation, Defence Forces, National Emergency Supply Agency, Ministry of Employment and the Economy, Security Police SUPO, Finnish Communications Regulatory Authority.

Timetable: A project plan will be ready in autumn 2009.

PROJECT 9: Measuring information security

Background/content of the measure:

Measuring information security is an umbrella project which will measure the success of the strategy and the development of information security in general. The project

will review how the level of information security is currently monitored in Finland and, based on this, a proposal will be made on available methods and mechanisms.

Performance/effectiveness target:

The project will establish the most effective possible implementation of the strategy. In addition, the project will determine indicators for the monitoring of national information security issues. The national view on the level of information security will be clarified and international comparability improved.

Implementation and monitoring responsibility:

Main responsibility: Petri Puhakainen /**The University of Oulu**
Participating: Statistics Finland, Finnish Communications Regulatory Authority, Microsoft, Ministry of Finance, Technical Research Centre of Finland VTT, Ministry of Transport and Communications, Defence Forces, Finnish Funding Agency for Technology and Innovation TEKES, Kesko, Nokia.

Timetable: An indicator survey will be ready in spring 2010.

6. IMPLEMENTATION, MONITORING AND RESOURCES

This action programme will implement the Government Resolution on National Information Security Strategy. Each project of the action programme has one organisation with leadership responsibility of the project in question (public or private sector party). The measures and monitoring necessary for implementing the strategy are specified in the action programme. More specific and more detailed measures, indicators and monitoring will be prepared in working groups during 2009.

The Ubiquitous Information Society Information Security Group, appointed by the Ministry of Transport and Communications, will support the harmonisation of measures required for implementing the strategy and will monitor implementation. Monitoring and supervision responsibility for the action programme will be affected such that the chairmen of the projects form a working committee. The committee will report on the progress of the work to the Ubiquitous Information Society Information Security Group.

The Ubiquitous Information Society Information Security Group will report to the Government annually on the implementation of the strategy and on the need to update the strategy, and will report to the Ubiquitous Information Society Advisory Board on the progress of the work. The Government has overall responsibility for information security strategy and it will supervise the implementation of the strategy and update it accordingly. The final reports of the projects will be completed by 28 February 2011, at which time the mandate of the Information Security Group under the Ubiquitous Information Society Advisory Board will expire.

The parties assuming leadership responsibility of the projects will be responsible for expenses arising in connection with the implementation of the action programme. The work for implementing the action programme will be carried out within the authorities' and officials' normal working hours. The R&D funds of the Ministry of Transport and Communications can be used for small-scale research projects by separate decision.